(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 47 374 A 1**

(51) Int. Cl.[7]:
H 04 L 9/00
H 04 L 12/22
H 04 B 1/38
H 04 B 7/26

(21) Aktenzeichen: 198 47 374.5
(22) Anmeldetag: 14. 10. 1998
(43) Offenlegungstag: 27. 4. 2000

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Hoffmann, Gerhard, Dipl.-Inform., 81547 München, DE; Lukas, Klaus, Dipl.-Inform., 81739 München, DE

(56) Entgegenhaltungen:

GB	21 88 514 A
EP	08 18 937 A1
JP	08-2 93 856 A
JP	08-18 657 A

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Anordnung zur verschlüsselten Übertragung von Information, Anordnung zur Entschlüsselung von über eine Funkverbindung übertragener verschlüsselter Information und System zur Übertragung von Information

(57) Anordnung zur verschlüsselten Übertragung von Information, Anordnung zur Entschlüsselung von über eine Funkverbindung übertragener verschlüsselter Information und System zur Übertragung von Information.
Der Einsatz einer Verschlüsselungseinheit in Verbindung mit einem mobilen Kommunikationsgerät ermöglicht eine Verschlüsselung und eine Entschlüsselung vor Ort. Ein Benutzer des Kommunikationsgeräts kann somit sicher sein, daß die von ihm versandten Daten schon verschlüsselt bzw. die empfgangenen Daten noch verschlüsselt sind.

DE 198 47 374 A 1

DE 198 47 374 A 1

BNSDOCID: <DE_____19847374A1_I_>

Beschreibung

Die Erfindung betrifft eine Anordnung zur verschlüsselten Übertragung von Information, eine Anordnung zur Entschlüsselung von über eine Funkverbindung übertragener verschlüsselter Information und ein System zur Übertragung von Information.

Eine Verschlüsselungseinheit ist aus [1] bekannt. Diese wird für beide Gesprächspartner eingesetzt. Die Verschlüsselungseinheit wird zwischen Telefon und Hörer angeschlossen. Im Betrieb ohne Verschlüsselung verhält sich die Verschlüsselungseinheit passiv, die Daten werden unverschlüsselt übertragen. Durch Druck auf eine Taste wird für beide Gesprächspartner die Verschlüsselung aktiviert. Die Verschlüsselungseinheit verwendet je Gespräch einen von 10^{38} Schlüssein. Über eine Anzeige wird eine aus dem Schlüssel abgeleitete Zufallszahl dargestellt. Diese Zufallszahl muß bei den Gesprächspartnern identisch sein, sie wird daher vorzugsweise vor dem eigentlichen Gespräch mündlich über die verschlüsselte Leitung ausgetauscht. Dadurch ist Sicherheit gewährleistet vor einem Mithörangriff auf der Leitung, bei dem ebenfalls zwei Verschlüsselungseinheiten eingesetzt werden.

Dabei ist es von Nachteil, daß eine derartige Verschlüsselungseinheit nur für Geräte am Festnetz erhältlich ist.

Ein symmetrisches Verschlüsselungsverfahren und ein asymmetrisches Verschlüsselungsverfahren (Public-Key-Verfahren) sind aus [2] bekannt.

Die Aufgabe der Erfindung besteht darin, über eine Funkverbindung eine verschlüsselte Übertragung von Information zu ermöglichen.

Diese Aufgabe wird gemäß den Merkmalen der unabhängigen Patentansprüche gelöst. Weiterbildungen der Erfindung ergeben sich auch aus den abhängigen Ansprüchen.

Zur Lösung der Aufgabe wird eine Anordnung zur Verschlüsselung von Information angegeben, bei der eine Eingabeeinheit vorgesehen ist, die derart eingerichtet ist, daß die Information von der Eingabeeinheit erfaßbar ist. Weiterhin ist eine Verschlüsselungseinheit (auch: Kryptoeinheit, Kryptoencoder) vorgesehen, mit der die erfaßte Information verschlüsselt wird. Mit einer Sendeeinheit wird diese verschlüsselte Information übertragen.

Bei der Information handelt es sich insbesondere um Sprache oder Daten, die analog oder digital übertragen werden.

Die Verschlüsselungseinheit ermöglicht eine Verschlüsselung mittels symmetrischem oder asymmetrischem Verfahren. Bei Einsatz des asymmetrischen Verfahrens ist ggf. eine Zertifizierungsinstanz zur Schlüsselverteilung (Trustcenter) vorzusehen, deren Vertrauenswürdigkeit zu gewährleisten ist.

Die Eingabeeinheit ist vorzugsweise ausgeführt als ein Mikrofon oder eine Digitalisiereinheit, bspw. ein Scanner. Auch kann die Eingabeeinheit ein Datenspeicher sein, aus dem die Information ausgelesen und an die Verschlüsselungseinheit übermittelt wird.

Insbesondere erfolgt die Übermittlung mittels der Sendeeinheit über ein Funknetz, z. B. ein GSM-Netz, ein DECT-Netz oder ein Satellitennetz.

Auch wird zur Lösung der Aufgabe eine Anordnung zur Entschlüsselung von über eine Funkverbindung übertragener verschlüsselter Information angegeben, bei der eine Empfangseinheit vorgesehen ist, die derart eingerichtet ist, daß die verschlüsselte Information empfangen wird. Weiterhin ist eine Verschlüsselungseinheit vorgesehen (auch: Kryptoeinheit, Kryptodecoder), die die empfangene verschlüsselte Information entschlüsselt. Mit einer Ausgabeeinheit erfolgt eine Ausgabe der entschlüsselten Information.

Die Ausgabe kann insbesondere an einen Lautsprecher, z. B. zur Ausgabe von Sprache, oder an einen Speicher, zum Ablegen digitaler Daten, erfolgen.

Hierbei sei angemerkt, daß die Daten sowohl analog als auch digitalisiert ausgegeben oder abgespeichert werden können. Es ist üblich, mittels Modem digitale bzw. digitalisierte Daten über analoge Leitungen zu übertragen. Dementsprechend kann die Umsetzung der analogen Sprache vorzugsweise innerhalb der Verschlüsselungseinheit in ein digitales Format erfolgen. Diese digitalisierten Daten werden einem Verschlüsselungsalgorithmus unterzogen und mit der Sendeeinheit als verschlüsselte Information zu mindestens einem Adressaten übertragen. Dort erfolgt eine Rückgewinnung (Entschlüsselung) der Information, z. B. der analogen Sprachdaten, aus den verschlüsselten Daten, indem diese mit der Verschlüsselungseinheit entschlüsselt werden und von ihrem digitalen Format in analoge Daten transformiert werden. Diese analogen Daten werden über eine Lautsprecher bei dem mindestens einen Adressaten ausgegeben. Die Umsetzung Verschlüsselung/Entschlüsselung erfolgt für einen Benutzer transparent, d. h. er nimmt den Dienst "sicheres Gespräch" wahr, ohne daß er dies merkt bzw. daß für ihn dadurch Nachteile im Vergleich zu einem normalen Telefongespräch entstehen. Dadurch erhöht sich die Akzeptanz bei dem Benutzer. Weiterhin kann er sicher sein, daß die Verschlüsselung der Daten vor Ort, also in dem Gerät erfolgt, das die Verschlüsselungseinheit enthält. Dies ist insofern von Bedeutung, als der Benutzer von der eigentlichen Verschlüsselung nichts bemerkt. Befindet sich das Gerät zur Ver-/Entschlüsselung bei ihm, kann er sicher sein, daß alles, was über die Sendeeinheit übertragen wird, bereits verschlüsselt wird. Eine Möglichkeit für einen Angriff auf die unverschlüsselte Information besteht jenseits der Sendeeinheit nicht. Dies führt zu einer hohen Benutzerakzeptanz.

Auch wird zur Lösung der Aufgabe ein System zur Übertragung von Information angegeben, das eine erste Anordnung zur verschlüsselten Übertragung von Information und eine zweite Anordnung zur Entschlüsselung von über eine Funkverbindung übertragener Information umfaßt.

Eine Ausgestaltung besteht darin, daß das System als ein Gerät ausgeführt ist. Insbesondere kann das Gerät mit einem Mobiltelefon (Handy) gekoppelt sein. Bei solch einer Kopplung wird bevorzugt eine an dem Mobiltelefon vorhandene Schnittstelle genutzt, die einen Anschluß des Mobiltelefons an eine Freisprecheinrichtung, z. B. zum Einsatz in einem Fahrzeug, vorsieht. Über diese Schnittstelle werden die Verbindungen zu Mikrofon und Lautsprecher des Mobiltelefons nach außen verfügbar gemacht, wobei insbesondere durch Anstecken eines Adapters an die Schnittstelle das interne Mikrofon und der interne Lautsprecher des Mobiltelefons abgeschaltet werden. Die Verbindung Lautsprecher/Mikrofon wird über eine Verschlüsselungseinheit mit einem Lautsprecher und einem Mikrofon des Geräts verbunden. Dadurch wird das Gerät wie das Mobiltelefon genutzt, wobei die Sprache über das Mikrofon des Geräts durch die Verschlüsselungseinheit verschlüsselt und umgekehrt verschlüsselte Information durch die Verschlüsselungseinheit entschlüsselt und als Sprache über den Lautsprecher des Geräts ausgegeben wird.

Im Rahmen einer zusätzlichen Ausgestaltung kann das Gerät in das Mobiltelefon integriert sein. Dadurch läßt sich eine handlichere Einheit aus Mobiltelefon und Gerät erzielen, die bei dem Benutzer auf eine entsprechend hohe Akzeptanz trifft.

Auch kann es insbesondere ein Vorteil sein, daß das Gerät portabel ausgeführt ist, da so der Benutzer in besonderen Fällen das Gerät koppelt und ggf. in unterschiedlichen Ein-

satzmöglichkeiten das Gerät flexibel mit verschiedenen Mobiltelefonen verbunden werden kann.

Ausführungsbeispiele der Erfindung werden nachfolgend anhand der Zeichnung dargestellt und erläutert.

Es zeigen

Fig. 1 eine erste Anordnung zur verschlüsselten Übertragung von Information;

Fig. 2 eine zweite Anordnung zur Entschlüsselung von über eine Funkverbindung übertragener verschlüsselter Information;

Fig. 3 ein System aus erster und zweiter Anordnung;

Fig. 4 eine Ausführungsmöglichkeit zur Kombination des Systems mit einem Mobiltelefon.

In **Fig.** 1 ist eine erste Anordnung **101** zur verschlüsselten Übertragung von Information **102** dargestellt. Bei der Information **102** handelt es sich insbesondere um Sprache oder Daten. Die Information **102** wird von einer Eingabeeinheit **103** aufgenommen, an eine Verschlüsselungseinheit **104** weitergeleitet und dort mittels eines vorgegebenen Verschlüsselungsalgorithmus verschlüsselt. Die verschlüsselte Information wird an eine Sendeeinheit **105** übermittelt und von dort als verschlüsselte Information **106** zu einem vorgegeben Adressaten über ein vorgegebenes Kommunikationsnetz, insbesondere ein Funknetz, übertragen.

Fig. 2 zeigt eine zweite Anordnung **201** als einen möglichen Adressaten der verschlüsselten Information **106**. Die verschlüsselte Information **106** wird von einer Empfangseinheit **202** aufgenommen und an eine Verschlüsselungseinheit **203** übermittelt. In der Verschlüsselungseinheit **203** erfolgt eine Entschlüsselung der verschlüsselten Information **106**. Die entschlüsselte Information **205** wird schließlich über eine Ausgabeeinheit **204**, vorzugsweise einen Lautsprecher, ausgegeben.

In **Fig.** 3 ist ein System aus erster und zweiter Anordnung (siehe hierzu **Fig.** 1 und **Fig.** 2) dargestellt. Die Information **102** wird über ein Mikrofon **302** als Eingabeeinheit **103** erfaßt und nach Verschlüsselung in der Verschlüsselungseinheit **104** über die Sendeeinheit **105** an ein Kommunikationsnetz **301** weitergeleitet. Das Kommunikationsnetz **301** ermöglicht eine Punktverbindung, bevorzugt über ein DECT-Netz, ein GSM-Netz oder eine Satellitenverbindung, zu einem Adressaten (vgl. zweite Anordnung **201**). Dort erfolgen Empfang (vgl. **202**), Entschlüsselung (vgl. **203**) und Ausgabe (vgl. **204**) der entschlüsselten Information **205** über einen Lautsprecher **303**.

Eine Ausführungsform einer möglichen Kombination des beschriebenen Systems in Form eines Geräts **409** mit einem Mobiltelefon **401** zeigt **Fig.** 4. Das Mobiltelefon **401** enthält einen Lautsprecher **402**, ein Mikrofon **403** und eine Schnittstelle **404**. Durch Anstecken eines dafür vorgesehenen Adapters an die Schnittstelle **404** werden Lautsprecher **402** und Mikrofon **403** überbrückt, d. h. stummgeschaltet, die Leitungen zu einem externen Mikrofon und einem externen Lautsprecher werden über die Schnittstelle **404** nach außen geführt.

Das Gerät **409** umfaßt einen solchen Adapter **405**, der mit der Schnittstelle **404** des Mobiltelefons **401** verbunden wird. In dem Gerät werden die Leitungen für Mikrofon und Lautsprecher mit einer Verschlüsselungseinheit **407** verbunden, dort erfolgt, wie oben beschrieben, eine Verschlüsselung von abgehender, d. h. über ein Mikrofon **408** aufgenommener, Information, bzw. eine Entschlüsselung eingehender, also über einen Lautsprecher **406** auszugebender Information. Als Sendeeinheit und Empfangseinheit wird das Mobiltelefon **401** genutzt.

Im Rahmen dieses Dokuments wurden folgende Veröffentlichungen zitiert:

[1] Siemens AG: "optiset E privacy module Hicom schützt Ihr Telefongespräch", Datenblatt 1/97, Siemens Aktiengesellschaft 1997, Bereich Private Kommunikationsnetze.

[2] Christoph Ruland: Informationssicherheit in Datennetzen, DATACOM-Verlag, Bergheim 1993, ISBN 3-89238-081-3, Seiten 42–46 und 73–85.

Patentansprüche

1. Anordnung zur verschlüsselten Übertragung von Information,
   a) bei der eine Eingabeeinheit vorgesehen ist, die derart eingerichtet ist, daß die Information von der Eingabeeinheit erfaßbar ist;
   b) bei der eine Verschlüsselungseinheit vorgesehen ist, die die erfaßte Information verschlüsselt und
   c) bei der eine Sendeeinheit vorgesehen ist, mit der die verschlüsselte Information übertragen wird.
2. Anordnung nach Anspruch 1, bei der die Eingabeeinheit ein Mikrofon, eine Digitalisiereinheit oder ein Datenspeicher ist.
3. Anordnung nach Anspruch 1 oder 2, bei der die Sendeeinheit eingerichtet ist zur Übertragung über ein Funknetz.
4. Anordnung zur Entschlüsselung von über eine Funkverbindung übertragener verschlüsselter Information,
   a) bei der eine Empfangseinheit vorgesehen ist, die derart eingerichtet ist, daß die verschlüsselte Information empfangen wird;
   b) bei der eine Verschlüsselungseinheit vorgesehen ist, die die empfangene verschlüsselte Information entschlüsselt und
   c) bei der eine Ausgabeeinheit vorgesehen ist, mit der die entschlüsselte Information ausgegeben wird.
5. Anordnung nach Anspruch 4, bei der die Ausgabeeinheit ein Lautsprecher oder eine Speichereinheit ist.
6. Anordnung nach Anspruch 5, bei der die Speichereinheit digital oder analog ausgeführt ist.
7. Anordnung nach einem der Ansprüche 1 bis 6, bei der die Information Sprache oder Daten umfaßt.
8. System zur Übertragung von Information
   a) mit einer ersten Anordnung zur verschlüsselten Übertragung von Information nach einem der Ansprüche 1 bis 3;
   b) mit einer zweiten Anordnung zur Entschlüsselung von über eine Funkverbindung übertragener verschlüsselter Information nach einem der Ansprüche 4 bis 6.
9. System nach Anspruch 8, das als ein Gerät ausgeführt ist.
10. System nach Anspruch 9, bei dem das Gerät mit einem Mobiltelefon (Handy) gekoppelt wird.
11. System nach Anspruch 10, bei dem das Gerät mit dem Mobiltelefon gekoppelt wird, indem das Gerät an der zum Freisprechen vorgesehenen Schnittstelle des Mobiltelefons angeschlossen wird.
12. System nach Anspruch 10, bei dem das Gerät in das Mobiltelefon integriert ist.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 198 47 374 A1
Int. Cl.[7]: H 04 L 9/00
Offenlegungstag: 27. April 2000

FIG 1

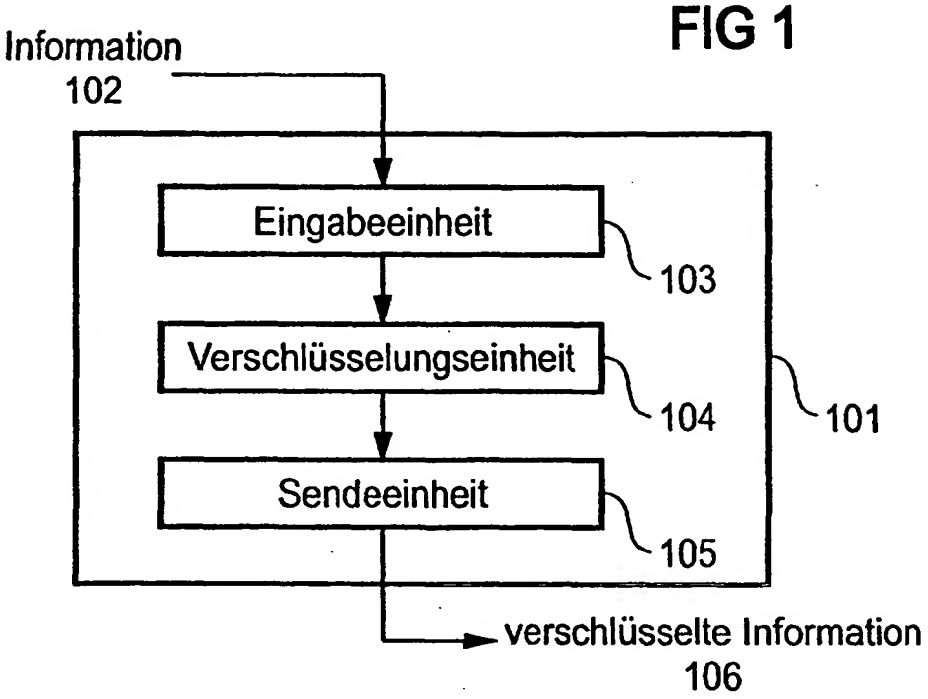
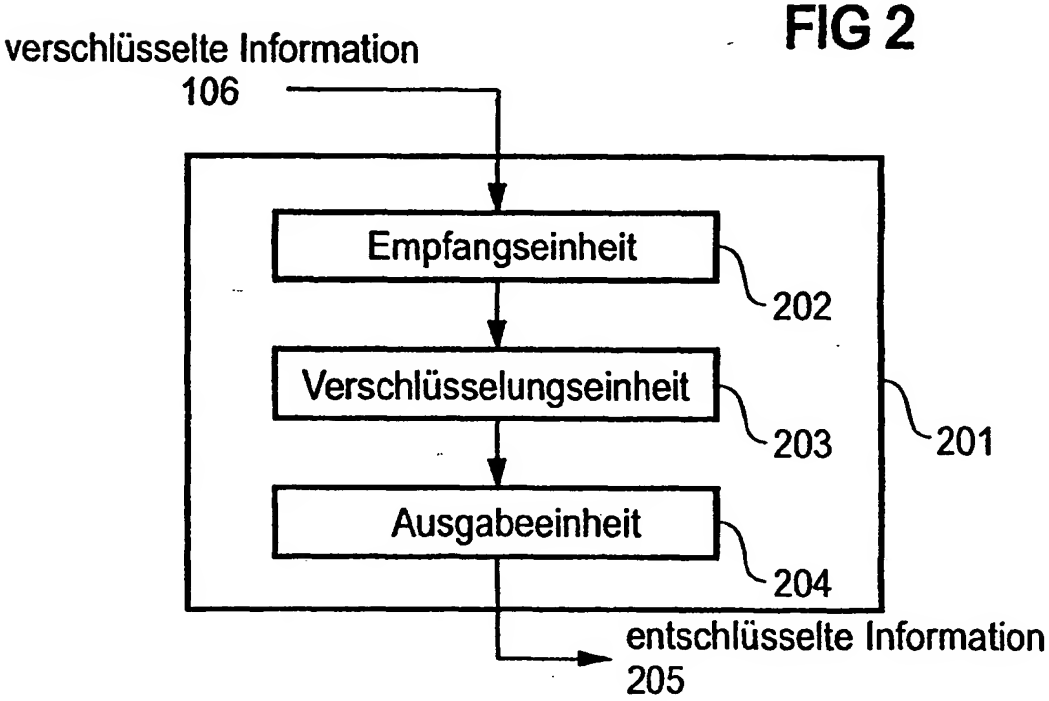


FIG 2



Nummer: DE 198 47 374 A1
Int. Cl.[7]: H 04 L 9/00
Offenlegungstag: 27. April 2000

FIG 3

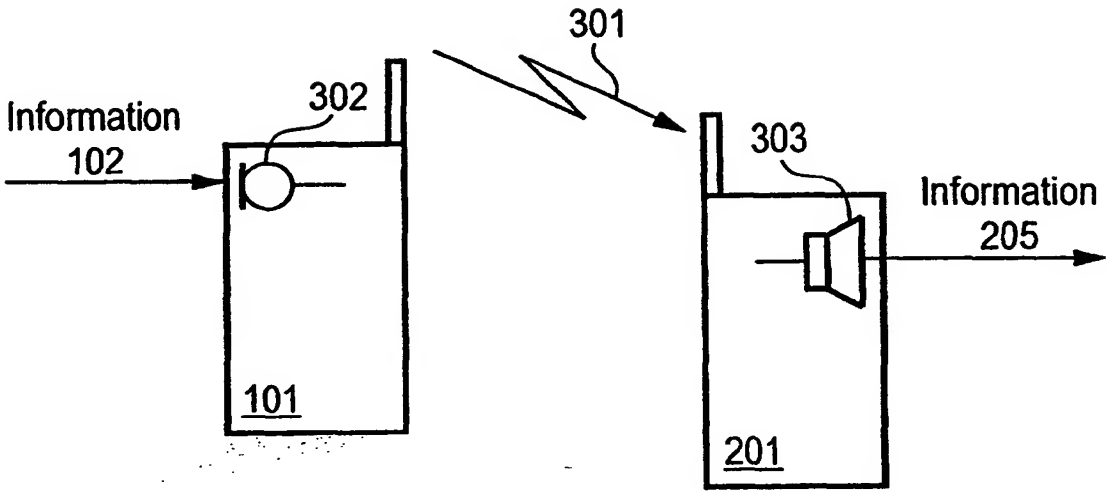


FIG 4